KEEPER | Pressemitteilung

Keeper Security empfiehlt zum ‘Change Your Password Day‘ ein starkes Credential-Management

Ein starkes Credential-Management ist für Unternehmen unerlässlich, um kritische Systeme zu schützen und unbefugten Zugriff auf sensible Daten zu verhindern.

München, 31. Januar 2025 – Keeper Security, ein führender Anbieter von Zero-Trust- und Zero-Knowledge Privileged Access Management (PAM)-Software zum Schutz von Passwörtern, Passwörtern, privilegierten Konten, Geheimnissen und Remote-Verbindungen, rät Unternehmen anlässlich des ‘Change Your Password Day‘, der Sicherheit von Zugangsdaten höchste Priorität einzuräumen. Durch die zunehmende Bedrohung durch Cyberangriffe und ohne angemessene Sicherheitsvorkehrungen können kompromittierte Anmeldedaten zu verheerenden Sicherheitsverletzungen, finanziellen Verlusten und Rufschädigung führen.

Privilegierte Konten, die häufig von Administratoren oder automatisierten Systemen für den Zugriff auf kritische Infrastrukturen verwendet werden, sind ein bevorzugtes Ziel der Angreifer, da sie umfassenden Zugriff auf die sensibelsten Systeme und Daten eines Unternehmens erlauben. Laut dem Verizon Data Breach Investigations Report 2024 sind fast 40 Prozent der Datenschutzverletzungen auf solche Konten zurückzuführen. Sicherheitsverletzungen, bei denen privilegierte Konten ausgenutzt werden, sind für die Opfer kostspielig: Laut einer Studie von IBM und dem Ponemon Institute schlägt der durchschnittliche Einbruch mit 4,35 Millionen Dollar zu Buche, während die Kosten für privilegierte Konten im Durchschnitt 4,5 Millionen Dollar betragen. Dies unterstreicht die dringende Notwendigkeit starker Sicherheitsmaßnahmen für Zugangsdaten.

„Schwache oder gestohlene Passwörter sind oft der erste und einfachste Einstiegspunkt für Cyberkriminelle. Anlässlich des ‘Change Your Password Day‘ möchten wir Unternehmen daran erinnern, wie wichtig es ist, solide Richtlinien für die Verwaltung von Anmeldeinformationen durchzusetzen“, sagt Darren Guccione, CEO und Mitbegründer von Keeper Security. „Die Implementierung von Tools wie Enterprise Password Management und Privileged Access Management stellt sicher, dass Anmeldeinformationen sicher gespeichert und verwaltet werden - inklusive einer Durchsetzung und Sichtbarkeit im gesamten Unternehmen. Derartige Tools minimieren das Risiko eines unbefugten Zugriffs, der zu einem schädlichen Einbruch führen kann.“

Da menschliches Versagen bei Sicherheitsverletzungen oft eine entscheidende Rolle spielt, ist die Information der Mitarbeiter über die besten Praktiken zur Passwortsicherheit von elementarer Bedeutung. Dazu gehören Schulungen zur Erkennung von Phishing-Versuchen, zur Vermeidung der Wiederverwendung von Passwörtern, zur Implementierung von MFA und zur Erkennung der Risiken bei der Weitergabe von Anmeldedaten über ungesicherte Kanäle. Da Unternehmen weiterhin hybride Arbeitsumgebungen managen müssen, ist die Sicherung von Anmeldedaten wichtiger denn je.

Keeper rät Organisationen zu:

- **Passwortrichtlinien implementieren**: Legen Sie eine Richtlinie fest und setzen Sie diese durch – beispielsweise, dass Passwörter eindeutig sind und mindestens 16 Zeichen mit Groß- und Kleinbuchstaben, Zahlen und Symbolen enthalten müssen.
- **Privileged Access Management (PAM)-Lösungen einsetzen**: Implementieren Sie PAM, um privilegierte Konten zu schützen, strenge Passwortrichtlinien durchzusetzen und den Zugang zu kritischen Systemen zu beschränken.
- **Multi-Faktor-Authentifizierung (MFA) erzwingen**: Fügen Sie mit MFA eine wichtige zusätzliche Sicherheitsebene hinzu, um Konten zu schützen, selbst wenn ein Passwort gefährdet ist.
- **Sicherheitsverletzungen überwachen**: Implementieren Sie eine Überwachung des Dark Web, um gefährdete Anmeldedaten zu erkennen.
- **Mitarbeiter schulen**: Führen Sie regelmäßige Schulungen zur sicheren Verwaltung von Anmeldeinformationen und zu bewährten Verfahren durch.

Der Verizon Data Breach Investigations Report 2024 bestätigt, dass 80 Prozent der Unternehmen, die PAM-Tools im Einsatz haben, einen signifikanten Rückgang der Erfolgsraten von Cyberangriffen im Zusammenhang mit dem Diebstahl und Missbrauch von Zugangsdaten verzeichnen. KeeperPAM® ist ein Teil der umfassenden Cybersecurity-Plattform von Keeper und bietet eine leistungsstarke Sicherung privilegierter Konten. Es sichert und verwaltet den Zugriff auf kritische Ressourcen wie Server, Webanwendungen, Datenbanken und Workloads. Als Cloud-native Zero-Knowledge-Plattform kombiniert KeeperPAM die Verwaltung von Unternehmenspasswörtern, Geheimnissen, Verbindungen, Zero-Trust-Netzwerkzugriff und Remote-Browser-Isolierung in einer benutzerfreundlichen Oberfläche. Von tausenden Organisationen vertraut und gestützt durch über 10 Jahre SOC-2-Compliance sowie Zertifizierungen nach ISO 27001, ISO 27017, ISO 27018 und FedRAMP-Autorisierung, bietet KeeperPAM eine sichere Grundlage zum Schutz kritischer Systeme und Daten. KeeperPAM erlaubt granulare, rollenbasierte Durchsetzungsrichtlinien, delegierte Administration und detaillierte Transparenz durch fortschrittliche Reporting-Tools. All dies trägt dazu bei, das Risiko der Kompromittierung von Anmeldeinformationen zu minimieren und Angreifer daran zu hindern, den Zugriff auszuweiten.

Zum ‘Change Your Password Day‘ am 1. Februar 2025 ermutigt Keeper alle Unternehmen zu proaktiven Schritten, um ihre digitalen Umgebungen zu sichern und ihr wertvolles Vermögen zu schützen.

###

Über Keeper Security:
Keeper Security verändert weltweit die Cybersicherheit für Menschen und Organisationen. Die intuitiven Lösungen von Keeper basieren auf einer End-to-End-Verschlüsselung, um jeden Anwender auf jedem Gerät und an jedem Standort zu schützen. Die Keeper Zero-Trust-Plattform für die Verwaltung von privilegierten Zugängen ist in wenigen Minuten einsatzbereit. Sie lässt sich nahtlos in jeden Technologie-Stack integrieren, um Sicherheitsverletzungen zu verhindern, Helpdesk-Kosten zu senken und Compliance zu gewährleisten. Keeper genießt das Vertrauen von Millionen von Einzelnutzern und Tausenden von Unternehmen und ist führend bei der Verwaltung von Passwörtern, Passkeys und Geheimnissen, privilegiertem Zugriff, sicherem Fernzugriff und verschlüsseltem Messaging. Erfahren Sie, wie die Zero-Trust- und Zero-Knowledge-Lösungen vor Cyber-Bedrohungen schützen auf KeeperSecurity.com.

Folgen Sie Keeper auf Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de